e-ISSN : 2620 3502
p-ISSN : 2615 3785

The emerging roles of Automation in safety and security

Alexander. P
[1]Siberian State Technological University, Siberia
Russian Federation
Email: alexander@list.ru

ABSTRACT

The present study defines automated solutions in safety and security in the emerging world. As there are large number of cyber security threats in the world there have been large number of solutions and one such solution is the use of automation in safety and security. Hence, the presented report display the role and importance of automation.

Keywords: automation, data, safety, security

INTRODUCTION

Security automation has been known as a machine-based execution of that of action to security along with that of power to be able to programmatically detect, remediate and investigate the threats of the cyber world that arise without or with human intervention by the identification of threats which are incoming by triaging and prioritising alerts as these arise and then by responding to the same in a timely manner. There are other things which security automation is able to accomplish such as detection of threats within an environment, triaging of potential threats by the following of certain step decision-making workflows instruction that will be taken by the analysts of security so as to be able to investigate the events and to determine whether it is an issue which is legitimate or not [1-5].

DISCUSSION

Security automation is also able to determine whether or not to take action in response to something that has happened and they may also be able to resolve and contain the issues. This could be happening in a matter of seconds without the requirement of action taken by the staff. Security automation is mostly used by the IT companies for IT departments of a company where security automation, time-consuming and repetitive activities are to be taken away from the hands of analysts security so they will be able to focus more on the value-adding and important parts of work. In addition to the following, security automation is also able to provide credit action which is rapid . According to research made by the ESG, IT teams have been ignoring 74% of the security alerts for events even though they have the proper solutions to security in place just because of the body of work. Security automation can not only be detecting and resolving common issues they are also able to eliminate human error which comes from work overload, negligence and inexperience. According to writer Aaron Hand, the terms security and safety are similar but not the same. Safety of the processes along with cybersecurity is deeply intertwined, having one type of accident easily infiltrating into the workings of another.

There has been widening prosperity that has been combining with that of the proliferation of sensors along with extensive connectivity through clouds which have accelerated the pace in which change takes place in systems of a factory along with their equipment. The ways by which factories are operating is really changing fast given the face of potent technological and economic forces. The government is concerned about that of dangerous and disrupted cybersecurity attacks that have been made on the plan along with the critical operations of infrastructure which are already collaborating with that of manufacturers along with the industrial operators. There are three sectors which have garnered the highest responses and they are for energy, critical manufacturing, wastewater and water. There are specific measures for mitigation of risk which organisations can be implementing and they will be depending on the unique set of risks security along with their potential impacts on that of safety. Every plant has to be segmented into zones which are a core security practice falling under the best practices. This can be used by every plant to be a part of their holistic defence-in-depth security approach so as to be able to help limit the access to systems of safety [5-12].

There is an industrial demilitarized zone also known as the IDMZ firewalls along with data brokers that may security segment the network plantwide from that of the network of the enterprise. There may also be used virtual LANs, also known as the VLAN along with a layer-3 and layer-2 for the hierarchy of switches so that they can create a functional sub-zone to be able to establish a smaller domain for the sake of simplifying security policy enforcement and for trust [10]. There are many organisations that are using RFID cards so that they are able to manage access controls to the same facility. However, the physical access of the security should be going further than this so as to be able to protect systems for safety. Block-out and lock-in devices can be utilised so as to be preventing the removal of cables which are unauthorised and so that they are able to close any unnecessary or unused ports. There is more advanced security for physical access that is coming up, such as that of the IP video surveillance system which may be using analytics so that faces are more recognisable.

There are ways of working together for devices incorporating CIP security CIP safety that may be helpful while protecting against the corruption of data along with attacks which are malicious on that of systems of safety. Companies are thinking about the usage of safety systems along with other hardware that should include security features that come built-in with it [8]. As an example it can be stated that safety controllers which use keep software may be able to ensure that firmware is downloaded only from a source that is trusted while the access door may be able to restrict physical access to that of the controller. A managed switch which is Industrial having list of access control or ACL may also be sure that devices which are authorised along with traffic and users are able to access a certain network. There are features of security software which will be able to restrict wireless and wired accesses to that of the infrastructure of a network. Companies are using authorisation and authentication security which is a primary element in the interface software connecting human to machines and they can limit the access to safety systems to that of individuals who are only authorised [10-14].

This is something which can help for the protection against that of accidental and malicious threats which occur internally. The companies hire security personnel who will be able to define who may be able to access a particular software and what kind of actions they will be able to perform and on which hardware specifically along with from where they will be able to perform these actions [6]. Management of assets and their software can be automated along with the discovery of acids that and you so that they are able to trap centrally and manage the changes of configuration across that of the entire facility which includes inside the systems of safety. These softwares are able to detect changes that are malicious in nature in real-time and they are able to log the activities along with reporting them to that of key personnel. This process includes having machinery in place so be able to immediately review the advisories and to determine the future impact. This may also include the implementation of procedures of patch management for that of effective products. Leveraging of automation may be able to contribute to that of orderly production in an environment and they can also secure the path of least resistance that of Engineers.

The above is believed by that of writer Patrick O’Doherty. The environment of production have become increasingly more complex and it is increasingly more difficult for that of a typical team of security to be able to safeguard everything manually [4]. The teams of security a struggling to be able to keep pace by using best practices which are old where is automation is seen as a key lever which may be able to enable the same teams to be performing their work efficaciously at scale. There is a growth in the ecosystem consisting of powerful tools that are built to be taking advantage of that of comprehensive APIs that is offered by providers of the cloud. This kind of automation makes it feasible to build solutions that are highly secure while ensuring that the team is able to move fast. From the top of a security aspect, automation are able to provide the two main benefits which are least-privilege isolation and reproducibility. The task which is automated can generate reproducible and identical results and that is very important since they create orderly and homogeneous production environment that can be significantly easier to be able to secure and manage.

So as to be able to not spend a lot of time giving special attention and care to every one of the servers one can be working with the same treating them to be a line-up of easily replaceable and disposable entities where any particular server is not utmost essential. There are some companies which have started provisioning manually along with the configuration of servers [2]. This is however lesser than the ideal since it can create constant risks of producing misconfigurations and inconsistencies through that of manual error. This is something that can be sounding not very serious at times however misconfigurations are tye reason why security incidents take place and these have been ranked as 6th on that of the 2017 OWASP list consisting of the 10 main applications that pose a security risk [9]. By the appropriate application of automation, one may be able to control the future sources of noise adequately as well as simultaneously evaluate risks of security along with minimisation of potential incidents that are caused by the updates which are not applied uniformly. Here are other benefits of automation as well such as the isolation of agents being made easier for that of executing tasks and using something that is known to be the principle of least privilege.

Clinging to the given context, there can be agents who may be anything from that of an engineer on the team to that of services of third-party software such as that of GitHub. One may also be the program which has been created so as to perform specific tasks [1]. The principle of that of least privilege can state that each of the agents should only be granted the minimum permissions sets that are required for the performance of their respective tasks. This is something which will not be feeling very familiar in the beginning however the applications are utmost commonplace in that of real life [5]. As an example, it can be said that it is highly unlikely that all employees within a company have been authorised so that they are able to be making wire transfers from that of the bank accounts of the company having a reason that is very sound. This approach has to be applied properly otherwise it can reduce any potential fallout as an agent is executed or compromised maliciously [7]. The reason behind the same being that attackers may have a personal scope for that of mischief which is curtailed by that of strict permissions to be granted to that of an agent who has compromised.

By that of appropriate isolation of agents, one can make it very difficult for that of an attacker who has compromised a production component from its environment which can be pivoting to a position that is more powerful where they will be able to gain either sensitive permissions or the access to that of a data set that is protected. A successful example is a company having manual processes for being able to provide the additional capacity of servers on that of the EC2 lying ahead which deploys new services along with that of automation which will be helpful for a change [3]. There are many cloud providers which offer sets of utilities of commands line that will be able to enable one to be performing actions by using the APIs from local terminals.

CONCLUSION

The essay tries to emphasize the fact that security is not just about the protection of data along with uptime. This is also about the protection of the environment along with people considering with the critical supplies and infrastructures on with the populace depends. Organisations which use automation at the ones that want to be staying ahead of success so that they can achieve compliance with that of the standard which is the latest along with holistically integrating security and safety. There are recent Automations which can also make risk analysis comprehensively along with implementing measures of risk mitigation using that of technology that is the latest.

REFERENCES

[1] Celik, Z. B., McDaniel, P., & Tan, G. (2018). Soteria: Automated iot safety and security analysis. In 2018 {USENIX} Annual Technical Conference ({USENIX}{ATC} 18) (pp. 147-158).

[2] Delsing, J. (Ed.). (2017). Iot automation: Arrowhead framework. CRC Press.

[3] A.V. Dastjerdi, H. Gupta, R.N. Calheiros, S.K. Ghosh, and R. Buyya. 2016. Chapter 4 - Fog Computing: principles, architectures, and applications. In Internet of Things, Rajkumar Buyya and Amir Vahid Dastjerdi (Eds.). Morgan Kaufmann, 61 -- 75.

[4] Driscoll, K. R., Roy, A., Ponchak, D. S., & Downey, A. N. (2017, March). Cyber safety and security for reduced crew operations (RCO). In 2017 IEEE Aerospace Conference (pp. 1-15). IEEE.

[5] Gupta, V., Mane, V., Pradhan, M. R., & Kotangale, K. B. (2017). IOT based car automation using Raspberry Pi. Imp. J. Interdiscip. Res.(IJIR), 3(4), 2454-1362.

[6] Aven, T. A unified framework for risk and vulnerability analysis covering both safety and security. Reliab. Eng. Syst. Saf. 2007, 92, 745–754.

[7] Plósz, S., Schmittner, C., & Varga, P. (2017, September). Combining safety and security analysis for industrial collaborative automation systems. In International Conference on Computer Safety, Reliability, and Security (pp. 187-198). Springer, Cham.

[8] Silva, N, Lopes, R. Practical Experiences with real-world systems: Security in the World of Reliable and Safe Systems. In Proceedings of the 2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), Budapest, Hungary, 24–27 June 2013; pp. 1–5

[9] Schoitsch, E., Schmittner, C., Ma, Z., & Gruber, T. (2016). The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles. In Advanced Microsystems for Automotive Applications 2015 (pp. 251-261). Springer, Cham.

[10] Śliwiński, M., & Piesik, E. (2017). Procedure based functional safety and information security management of industrial automation and control systems on example of the oil port installations. In Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars (Vol. 8, pp. 129-137).

[11] Varga, P., Plosz, S., Soos, G., & Hegedus, C. (2017, May). Security threats and issues in automation IoT. In 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS) (pp. 1-6). IEEE.

[12] Wendzel, S., Tonejc, J., Kaur, J., Kobekova, A., Song, H., Fink, G. A., & Jeschke, S. (2017). Cyber security of smart buildings. Wiley.

[13] SM. Mohammad and Lakshmisri, Surya, Security Automation in Information Technology (June 1, 2018). INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT) – Volume 6, Issue 2 - June 2018,

[14] SM.Mohammed. 2017.DevOps Automation and Agile Methodology. International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 3, pp.946-949,